Privacy Year in Review: Developments in HIPAA

ELIZABETH HUTTON & DEVIN BARRY*

ABSTRACT

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA). A key motivation behind the passage of this bill was to preserve the confidentiality of an individual's protected health information. To accomplish this aim, Congress empowered the Department of Health and Human Services to promulgate regulations governing when and to what extent an individual's health information may be disclosed. These regulations become collectively known as the Privacy Rule and carry severe penalties for their violation. Since its compliance date of April 14, 2003, numerous concerns have arisen regarding the efficacy and implications of the Rule. This article addresses the following four questions: 1) whether the Privacy Rule is actually being enforced, 2) whether the Department of Justice is empowered to prosecute individuals, not just covered entities, for violations of the Rule, 3) the extent to which the Privacy Rule protects genetic information and its implications for the future of genetic privacy, and 4) how the Privacy Rule interacts with other federal and state laws addressing the privacy of health information.

I. INTRODUCTION

A key motivation behind the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was to preserve the confidentiality of an individual's protected health information. Through HIPAA, Congress empowered the Department of Health and Human Services (HHS) to issue regulations governing how, when, and to what extent private health information may be disclosed. These regulations, known collectively as the Privacy Rule, had a compliance date of April 14, 2003 for most covered entities and since that date, numerous questions and concerns have arisen concerning the Rule's scope, interpretation, and implications.[1] This article will address the following: 1) whether the Privacy Rule is actually being enforced, 2) whether the Department of Justice is empowered to prosecute individuals, not just covered entities, for violations of the Privacy

* Devin Barry and Elizabeth Hutton are candidates for juris doctor at The Ohio State University Moritz College of Law, class of 2006. Devin Barry has a B.S. in management information systems from Miami University of Ohio. Elizabeth Hutton holds a B.A. in government from Harvard College.

[1] Privacy Rule, 45 C.F.R. § 164 (2005).

Rule, 3) the extent to which the Privacy Rule protects genetic information and its implications for the future of genetic privacy, and 4) how the Privacy Rule interacts with other federal and state laws addressing the privacy of health information.

II. HIPAA: A BEGINNER'S GUIDE

A. WHY WAS HIPAA ENACTED?

HIPAA[2] was enacted to reduce the monetary cost of administrative operations in the health care industry and to simplify the exchange of electronic health information, with particular focus on preventing fraud and unauthorized access to, and disclosure of, individually identifiable health information.[3] To accomplish this goal, Congress incorporated into HIPAA sections 261 through 264, known collectively as the "Administrative Simplification" provisions. These provisions empower HHS to create and publish rules to streamline the electronic exchange of health information.[4] At the same time, Congress recognized that advances in electronic technology could seriously threaten patient privacy, and included in the Administrative Simplification provisions explicit authority for HHS to adopt rules to protect the confidentiality of individually identifiable health information.[5]

B. WHAT IS A COVERED ENTITY?

HIPAA applies to three particular categories of persons, known as "covered entities."[6] Section 1172(a) of the statute reads, in relevant part, "any standard adopted under this part shall apply, in whole or in part, to the following persons: . . . 1. a health plan . . . 2. a health care clearinghouse . . . 3. a health care provider who transmits any health information in electronic form in connection with a transaction

---

[2] Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191,110 Stat. 1936 (1996), http://aspe.hhs.gov/admnsimp/pl104191.htm.

[3] *Id.* pmbl.

[4] HIPAA § 1173.

[5] HIPAA § 264.

[6] HIPAA § 1172.

referred to in section 1173(a) (1)."[7] Each of the three entities is defined in detail in the statute.[8] If an entity is not a covered entity as defined in the statute, it is presumably not required to comply with the Administrative Simplification provisions or any regulations promulgated there under by HHS.

Ascertaining whether an entity is covered by HIPAA can be a vexing determination, particularly because the language of the statute is so complex. There are numerous resources available online that can assist an entity in determining whether it is covered, including a "Covered Entity Decision Tool" provided by the Center for Medicare and Medicaid Services.[9]

C. THE ADMINISTRATIVE SIMPLIFICATION PROVISIONS

HIPAA's Administrative Simplification provisions are divided into four sections: 1) Electronic Transactions and Code Sets, 2) Unique Identifiers, 3) Security, and 4) Privacy. Each of these four provisions is activated when HHS issues a final set of regulations, known as a final rule.[10] Each final rule will list a particular compliance date (these dates are different for each provision because HHS releases final regulations as they are developed) by which covered entities must meet the rules' requirements.

1. TRANSACTIONS AND CODE SETS

In the past, the health care industry, including health care providers and insurance plans, used different electronic formats and definitions of data elements to process medical claims. As a result, data had to be

---

[7] HIPAA § 1173(a)(1): The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for— (A) the financial and administrative transactions described in paragraph (2); and (B) other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs.

[8] For definitions of: "health plan," see HIPAA § 1171(5); "health care clearinghouse," see HIPAA § 1171(2); "health care provider," see HIPAA § 1171(3).

[9] The Covered Entity Decision Tool may be accessed at http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp (last visited Mar. 20, 2005). *See also* http://www.hipaacomply.com/coveredentity_faq.htm (last visited Feb. 21, 2005).

[10] HIPAA Primer, *at* http://www.hipaadvisory.com/regs/HIPAAprimer.htm (last visited Feb. 20, 2005).

reformatted and recoded before it could be shared, resulting in high administrative costs. By ordering a standardized transaction and code system, Congress intended to reduce handling and processing time, to improve data quality, and to decrease administrative costs.

Section 1173(a)(1) of HIPAA states that "the Secretary [of HHS] shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically."[11] On April 17, 2000, HHS released the final rule governing electronic transactions and code sets.[12] Compliance with this rule was required by October 16, 2002 for large health plans, health care providers, and health care clearinghouses, while small health plans[13] had until October 16, 2003 to comply. However, in December 2001, Congress enacted the Administrative Simplification Compliance Act (ASCA),[14] which granted a one-year compliance extension to October 16, 2003. In February 2003 HHS modified the final rule,[15] but the compliance date of October 16, 2003 for all covered entities was unchanged.[16]

2. IDENTIFICATION STANDARDS

As was the case with transactions and code sets, the health care industry used multiple identification formats when engaging in business transactions with each other. For example, employers often used different identifiers (for example, a health care provider, patient, or patient's employer might be referred to by several different names: John Doe, John J. Doe, John Doe Jr., etc.) when communicating with

---

[11] HIPAA § 1173(a)(1).

[12] 45 C.F.R. §§ 160 and 162 (2005), http://www.cms.hhs.gov/hipaa/hipaa2/regulations/transactions/finalrule/txfinal.pdf (last visited Feb. 20, 2005).

[13] A "small health plan" is a health plan with annual receipts of $5 million or less. 45 C.F.R. § 160.103.

[14] Administrative Simplification Compliance Act, Pub. L. No. 107-105, 115 Stat. 1003 (2001), http://www.hipaadvisory.com/regs/regs_in_PDF/asca.pdf (last visited Feb. 20, 2005).

[15] Health Insurance Reform: Modifications to Electronic Data Transaction Standards and Code Sets, 68 Fed. Reg. 8381 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 162), *at* http://www.hipaadvisory.com/regs/finaltransmod/finaltransmod.txt (last visited Feb. 20, 2005).

[16] For more information on the transaction and code sets rule, see http://www.hipaadvisory.com (last visited Feb. 20, 2005).

health plans, which was inefficient and confusing. In section 1173(b)(1) of HIPAA, Congress authorized HHS to adopt standard unique health identifiers for every individual, employer, health plan, and health care provider participating in the health care system,[17] which are intended to reduce errors and administrative costs.[18]

HHS published the final rule on January 23, 2004.[19] The effective date of the rule is May 23, 2005, with a compliance deadline of May 23, 2007 (May 23, 2008 for small health plans). After that date, any covered entity that transmits health information in electronic format must comply with this rule.[20]

3. SECURITY STANDARDS

While a main goal of HIPAA's Administrative Simplification provisions is to reduce errors and administrative costs, Congress was also concerned with the security of electronically transmitted health data. Section 1173(d) of those provisions empowers HHS to adopt regulations to ensure the integrity and confidentiality of electronic protected health information.[21]

The final security standards were published on February 20, 2003 with an effective date of April 21, 2003.[22] The final rule requires covered entities to take certain precautions to secure health information created, received, maintained, or transmitted by that entity and to protect against reasonably anticipated threats or hazards to the security of certain protected health information.[23] The rule requires that adequate security measures be in place to protect networks, computers, and other electronic devices used in transmitting or storing

---

[17] HIPAA of 1996, Pub. L. No 104-191, § 1173(b)(1), 110 Stat. 1936, 2025 (1996).

[18] 45 C.F.R. § 162 (2005), http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2004/pdf/04-1149.pdf (last visited Feb. 20, 2005).

[19] *Id.*

[20] For more information on the identification standards, see http://www.cms.hhs.gov/hipaa/hipaa2/regulations/identifiers/default.asp (last visited Feb. 20, 2005). *See also* www.hipaadvisory.com (last visited Feb. 20, 2005).

[21] HIPAA § 1173(d).

[22] 45 C.F.R. § 164, http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf (last visited Feb. 20, 2005).

[23] HIPAA Primer, *supra* note 10.

electronic protected health information.[24] For example, individuals must be assigned unique passwords in order to access confidential information electronically, and the system must keep a record of who viewed what information so that it is possible to check whether all individuals who accessed a specific record had an appropriate need to know. Most covered entities will have until April 21, 2005 to comply with the security standards (April 21, 2006 for small health plans).[25]

4. THE PRIVACY RULE

Section 264 of the Administrative Simplification provisions authorizes HHS to promulgate privacy regulations for individually identifiable health information (IIHI), also known as protected health information, or PHI, used by covered entities. The final regulations would become known as the "Privacy Rule."

A primary goal of the Privacy Rule is to "define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities."[26] IIHI is a subset of health information that either identifies the individual, or provides a reasonable probability that the information could be used to identify the individual.[27] Examples of IIHI range from the obvious like name, address, birthdate, and social security number to less obvious information like a credit card number, telephone number, or even the name of an individual's obstetrician.

The Privacy Rule contains several provisions of particular interest to patients and health care providers. The Rule protects an individual's right to access his or her protected health information[28] by dictating that a covered entity must allow individuals "access to inspect and obtain a copy of protected health information about the individual."[29]

---

[24] *Id.*

[25] For more information on the Security Rule, see http://www.hipaadvisory.com (last visited Feb. 20, 2005).

[26] OFFICE FOR CIVIL RIGHTS, U.S. DEPT. OF HEALTH & HUMAN SERVICES, SUMMARY OF THE HIPAA PRIVACY RULE 4 (2003), *available at* http://www.hhs.gov/ocr/privacysummary.pdf (last visited Feb. 20, 2005).

[27] 45 C.F.R. § 160.103.

[28] For a definition of "protected health information," see 45 C.F.R. § 160.102.

[29] 45 C.F.R. §164.524.

The Rule directs covered entities to provide a notice of privacy practices to patients so they understand "the uses and disclosures of protected health information that may be made by the covered entity . . . and the covered entity's legal duties with respect to protected health information."[30] The Privacy Rule requires covered entities to adhere to a minimum necessary standard when disclosing protected health information.[31] "Minimum necessary" means that when disclosing protected health information, a covered entity must make "reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."[32]

Of particular interest to covered entities are the administrative regulations contained within the Privacy Rule. Among other requirements, these provisions mandate that a covered entity train all members of its workforce about protected health information,[33] that it designate a privacy official responsible for the implementation of the Privacy Rule,[34] that it provide for sanctions against an employee who fails to comply with the Privacy Rule,[35] and that a covered entity have procedures for individuals to complain about any failure to adhere to the Privacy Rule.[36]

HHS published the Privacy Rule on December 28, 2000, with an effective date of April 14, 2001. However, the rule was modified to ensure that it functioned as intended, and in August 2002, HHS adopted a modified final version of the Privacy Rule. By the compliance date of April 14, 2003 (April 14, 2004 for small health

---

[30] 45 C.F.R. § 164.520(a)(1). For more information on the notice requirement, see http://www.hhs.gov/ocr/hipaa/guidelines/notice.pdf (last visited Feb. 20, 2005).

[31] 45 C.F.R. § 164.502(b).

[32] 45 C.F.R. § 164.502(b)(1). For more information on the minimum necessary standard, see http://www.hhs.gov/ocr/hipaa/guidelines/minimumnecessary.pdf (last visited Feb. 20, 2005).

[33] 45 C.F.R. § 164.530(b)(1).

[34] 45 C.F.R. § 164.530(a)(1)(i).

[35] 45 C.F.R. § 164.530(e)(1).

[36] 45 C.F.R. §§ 164.530(a)(1)(ii) and (d)(1).

plans), covered entities must have fully implemented the Privacy Rule.[37]

5. ENFORCEMENT OF HIPAA'S ADMINISTRATIVE SIMPLIFICATION PROVISIONS

HIPAA's Administrative Simplification provisions authorize the imposition of civil and criminal penalties (including jail time) for failure to abide by the final rules adopted by HHS. Section 1176, entitled "General Penalty for Failure to Comply with Requirements and Standards," empowers the Secretary of Health and Human Services to impose a penalty of not more than $100 per violation and limits the total penalty that may be imposed on a person for all violations of an identical requirement during a calendar year to not more than $25,000.[38] HHS is responsible for assessing civil monetary penalties for violations of the Administrative Simplification provisions, while responsibility for investigation and enforcement of the Privacy Rule in particular is assigned to the Office for Civil Rights (OCR), a division of HHS.[39]

HIPAA specifically permits criminal penalties for "wrongful disclosure of individually identifiable health information."[40] Section 1177 outlines a three-tiered punishment scale for "a person who knowingly . . . uses or causes to be used a unique health identifier [or] obtains individually identifiable health information relating to an individual or discloses individually identifiable health information to another person."[41] For the least serious violations, the individual may be fined up to $50,000 and/or imprisoned for not more than one year. If the offense is committed under false pretenses, the fine increases to not more than $100,000 and/or not more than five years imprisonment. But if the offense is committed for personal gain or malicious harm, the penalty increases to a fine of not more than $250,000 and/or

---

[37] 45 C.F.R. § 164.534. For more information on the Privacy Rule, see the OCR website at http://www.hhs.gov/ocr/hipaa/ (last visited Feb. 20, 2005). *See also* http://www.hhs.gov/ocr/privacysummary.pdf (last visited Feb. 20, 2005).

[38] HIPAA of 1996, Pub. L. No. 104-191, § 1176, 110 Stat. 1936, 2028-29.

[39] 45 C.F.R. § 160.

[40] HIPAA § 1177.

[41] HIPAA § 1177(a).

imprisonment for not more than ten years.[42] Congress delegated criminal enforcement of HIPAA's Administrative Simplification provisions to the United States Department of Justice (DOJ).[43]

III. IS THE OFFICE FOR CIVIL RIGHTS ENFORCING THE PRIVACY RULE?

A. GENERAL EXPLANATION OF THE ISSUE

As of July 31, 2004, the Office for Civil Rights had received and initiated investigations of 7,577 complaints alleging violations of the Privacy Rule. Fifty-seven percent of those cases were closed as of July 31 and over one hundred have been referred to the Department of Justice as possible criminal violations.[44] OCR estimates that it receives over one hundred privacy-related complaints per week.[45] Most of the complaints involve 1) impermissible disclosure of health information, 2) absence of sufficient safeguards to prevent impermissible use of health data, 3) failure to allow patients access to their medical records, 4) violations of the minimum necessary standard for disclosure of health information, and 5) disclosure of health information without proper authorization.[46] To date, OCR has not imposed any civil monetary penalties.

B. WHY HASN'T THE OCR ASSESSED CIVIL MONETARY PENALTIES?

OCR's enforcement strategy focuses on voluntary compliance and education rather than punishment.[47] On April 17, 2003, three days before the Privacy Rule became effective, HHS issued the first installment of an enforcement rule, which "establishes rules of

---

[42] HIPAA § 1177(b).

[43] OFFICE FOR CIVIL RIGHTS, *supra* note 26.

[44] Shannon Hartsfield, *Health Law Alert: A HIPAA Wake-Up Call*, HEALTH LAW ¶ 5 (Holland + Knight LLP), Aug. 24, 2004 *at* http://www.hklaw.com/Publications/Newsletters.asp?IssueID=488&Article=2676 (last visited Feb. 20, 2005).

[45] Gregory Frost, *Are the Enforcers Enforcing?*, 6 ORTHOPEDIC TECH. REV. 7, ¶ 3 (Mar./Apr. 2004) *at* http://www.orthopedictechreview.com/issues/marapr04/pg41.htm (last visited Feb. 20, 2005).

[46] Hartsfield, *supra* note 44.

[47] 45 C.F.R. § 160(II) (2005).

procedure for the imposition, by the Secretary of Health and Human Services, of civil money penalties on entities that violate standards adopted by the Secretary under the Administrative Simplification provisions."[48] In its preamble, the rule states that the official approach to violations and enforcement is to work cooperatively with covered entities to obtain compliance voluntarily and informally before pursuing formal enforcement.[49] This suggests that OCR's strategy is to educate first and penalize as a last resort. This interim enforcement rule ceases to be in effect on September 16, 2005. Additional enforcement rules are forthcoming.[50]

In 2004, OCR Director Richard Campanelli emphasized this cooperative approach, stating that it "has always been, and continues to be, that the most effective means of obtaining compliance is through voluntary compliance."[51] Campanelli further explained that when allegations of a privacy rule violation surface, OCR "get[s] in touch with 'the covered entity' and let[s] them know the allegation. If it's true, quickly the covered entity comes into compliance with the rule and it is an opportunity for us to educate."[52]

In 2003, Susan McAndrew, OCR's Senior Advisor for HIPAA Privacy Policy, indicated that covered entities who may be in violation of the Privacy Rule have been cooperative and responsive, making the imposition of civil monetary penalties unnecessary. In a September 2003 speech, McAndrew asserted that "we haven't . . . in the first five months, had an occasion to [impose any fines]." She went on to say that OCR would do so "only if we find a covered entity is recalcitrant."[53] This comment suggests that to date, most covered entities against whom there have been credible allegations of privacy violations have satisfactorily addressed the problem to prevent future infractions.

---

[48] 45 C.F.R. § 160.

[49] *Id.*

[50] *Id.*

[51] Nina Youngstrom, *OCR Chief Sees HIPAA Confusion Waning, But Complaints Persist*, REPORT ON MEDICARE COMPLIANCE (Atlantic Info. Services, Inc., Washington, D.C.), June 2004, *at* http://www.aishealth.com/Compliance/Hipaa/RMCConfusionWaningComplaints.html (last visited Feb. 20, 2005).

[52] *Id.*

[53] Frost, *supra* note 45 ¶ 8.

OCR may have chosen not to impose civil monetary penalties to date for violations of the Privacy Rule because it can only assign such penalties under appropriate circumstances. Richard Campenelli testified that Congress has only allowed HHS to impose civil penalties if the covered entity "did not know, and by exercising reasonable diligence would not have known, of the violation . . . . If failure to comply was due to reasonable cause and not willful neglect, and the entity corrects the violation within thirty days of when it knew or should have known of the error," OCR will not impose penalties.[54]

A third consideration is that HHS has yet to release a finalized version of the enforcement rule. The interim rule, which expires on September 16, 2005, offers some temporary guidance, but until there is a final rule, covered entities are not put on notice as to how HHS intends to enforce its regulations. If OCR were to levy civil monetary penalties for a violation of the Privacy Rule before a final enforcement rule is published, they would in all likelihood be challenged in court for lacking statutory authority.[55] Once a final version of the enforcement rule is released, HHS would have the necessary statutory authority to impose civil monetary fines, and covered entities would have fair notice of what is expected of them. Until those guidelines are released, OCR may be hesitant to impose penalties.

In assessing why OCR has not imposed any civil penalties, an important consideration is the quality and legitimacy of the privacy complaints that OCR has received. To date, OCR has rejected fifty-five percent of privacy complaints for either lack of jurisdiction or, if the allegations in the complaints were to be proven true, they still would not constitute violations of the Privacy Rule.[56] Some of the complaints seem to result from a misunderstanding of the extent of protection provided by the Privacy Rule. Candace Foster, HIPAA team leader at Deaconess Hospital in Evansville, Indiana observes that patients have a misperception that HIPAA "provides ironclad

---

[54] *HIPAA Medical Privacy and Transaction Rules: Overkill or Overdue? Before the Senate Spec. Comm. on Aging*, 108th Cong. ¶ 25 (2003) (statement of Richard Campanelli, Director, Office for Civil Rights, U.S. Dept. of Health & Human Services), *at* http://www.hhs.gov/asl/testify/t030923.html (last visited Feb. 20, 2005).

[55] Ronald J. Levine et al., *The Evolving Protections of HIPAA Regulations*, N.Y.L.J., Aug. 30, 2004, at 9.

[56] Patty Enrado, *More HIPAA Complaints to Come in 2005*, HEALTHCARE IT NEWS, Oct. 2004, at ¶ 5, *at* http://www.healthcareitnews.com/NewsArticleView.aspx?ContentID=1648&ContentTypeID=3&IssueID=11 (Last accessed on 2/20/05).

guarantees of privacy at all times . . . . I hear people say 'this is in violation of HIPAA' - but it's not."[57] This large percentage of non-actionable complaints helps explain why OCR has not imposed any civil penalties to date.

While a large percentage of complaints are not actionable for lack of jurisdiction or no violation, a number of complaints are filed maliciously. According to the January 2005 "Report on Patient Privacy," a monthly newsletter published by Atlantic Information Services (AIS), "HIPAA has become the latest vehicle of catty and even malicious patients and employees, who file phony privacy complaints to hurt others," although the author cautions that "it's unclear how widespread the phenomenon is."[58] Kelley Meeusen, Health Information Compliance Coordinator and Privacy Officer at Harrison Hospital in Bremerton, Washington, points out that of sixteen privacy complaints that have been filed against it since April of 2003, only four were found to be valid. In fact, the only complaint that triggered an OCR investigation was found to be a phony privacy complaint filed by a patient.[59]

Attorney Leslie Bender confirms that some privacy complaints are motivated, at least in part, by vengeful purposes. While assessing the effectiveness of a Maryland hospital's HIPAA policies, Bender discovered that angry employees threatened to file complaints with OCR to force out a new manager.[60] According to Bender, during a conversation with hospital employees about a new manager, one stated that they "had HIPAA dirt on her and if she didn't get better at her job, they'd file complaints with OCR and force her out."[61] While the legitimacy of these particular employees' complaints regarding privacy violations is unknown, it seems that the Privacy Rule is being used to wage personal vendettas and at least some of these complaints are baseless.

---

[57] Nina Youngstrom, *Some Patients and Employees Misuse HIPAA in Personal Attacks*, REPORT ON PATIENT PRIVACY (Atlantic Info. Services, Inc., Washington, D.C.), Jan. 2005, *at* http://www.aispub.com/Bnow/011905e.html (last visited Feb. 20, 2005).

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *Id.*

C. A MOVE TOWARDS MORE AGGRESSIVE ENFORCEMENT?

While OCR has not chosen to impose civil monetary penalties to date, some legal experts believe that it is making a move towards more visible enforcement. In a 2004 presentation before the Health Law Section of the District of Columbia Bar, OCR Director Richard Campanelli indicated that a number of both civil and criminal complaints involving Privacy Rule violations are "in the pipeline" for enforcement.[62] The number of complaints in the pipeline has been estimated to be around sixty.[63] Attorney Kirk J. Nahra of the Wiley Rein & Fielding Privacy Practice predicts that while covered entities generally make good faith efforts to come into compliance, "we can expect more aggressive enforcement of rules over the next year"[64] and advises covered entities to "remain vigilant in their compliance activities."[65] Gloria Steinberg of the Southern Healthcare Administrative Regional Process (SHARP) and the Workgroup for Electronic Data Interchange (WEDI) estimates that "once enough of the final rules are released and all stakeholders become better educated . . . a plethora of HIPAA complaints [will] be filed in 2005."[66]

IV. DOJ "WARNING SHOT"? – *UNITED STATES V. GIBSON*[67]

A. CASE SUMMARY

In October 2003 phlebotomist Richard W. Gibson of SeaTac, Washington impermissibly disclosed cancer patient Eric Drew's individually identifiable health information to several credit card companies to obtain four credit cards in Drew's name.[68] Specifically,

---

[62] Kirk J. Narha, *A New Era for HIPAA Enforcement*, PRIVACY IN FOCUS (Wiley Rein & Fielding, Washington, D.C.), Mar. 2004, *at* http://www.wrf.com/publications/publication.asp?id=83556632004 (last Feb. 20, 2005).

[63] Youngstrom, *supra* note 51.

[64] Narha, *supra* note 62.

[65] *Id.*

[66] Enrado, *supra* note 56.

[67] DOJ Complaint against Richard Gibson *at* http://www.usdoj.gov/usao/waw/press_room/2004/aug/pdf_files/cr04_0374rsm_inf.pdf (last visited Feb. 20, 2005).

[68] *Id.* at 2.

Gibson disclosed Drew's name, date of birth, and social security number, all protected health information, which had been collected by Gibson's employer, the Seattle Cancer Care Alliance, for payment of health care services.[69] Gibson charged more than $9,000 for items including "video games, home improvement supplies, apparel, jewelry, porcelain figurines, groceries and gasoline."[70] After his employer discovered that Gibson had abused his position to obtain and misuse protected health information, he was fired.

The Department of Justice charged Gibson, as an individual, with wrongful disclosure of individually identifiable health information under 42 U.S.C. § 1320(d) (6) of HIPAA. The government and Gibson entered into a plea agreement, which was accepted by the court. Calling his actions "some of the most deplorable [behavior] I've seen in 15 years on the bench,"[71] on November 5, 2004, U.S. District Court Judge Ricardo S. Martinez sentenced Gibson to sixteen months in prison, four months longer than requested by the prosecution, and ordered him to pay at least $15,000 in restitution in the first criminal prosecution under HIPAA.[72]

The prosecution was unexpected to some because HIPAA specifically states that it only applies to covered entities and not to non-covered individuals like Gibson. HHS has consistently stated that it is only permitted by statute to impose privacy standards on a covered entity, "not business associates, not employers and not individuals who are not themselves CEs."[73] Gibson presumably did not handle the electronic transmission of protected health information and therefore would not meet the definition of "health care provider" under HIPAA, and would not be a covered entity within the meaning of the statute. The decision to prosecute Gibson has led some to question the legality of enforcing HIPAA against non-covered individuals and the implications of doing so.

---

[69] *Id.*

[70] Gibson Plea Agreement at 6, *at* http://www.usdoj.gov/usao/waw/press_room/2004/aug/pdf_files/cr04_0374rsm_plea.pdf (last visited Feb. 20, 2005).

[71] Gene Johnson, *Seattle Technician Sentenced in Identity Theft*, THE COLUMBIAN, Nov. 6, 2004, at c2.

[72] *Id.*

[73] Nina Youngstrom, *Are Individuals Covered by HIPAA? If So, What Would It Mean for Covered Entities?*, REPORT ON PATIENT PRIVACY (Atlantic Info. Services, Inc., Washington, D.C.), Oct. 2004, *at* http://www.aishealth.com/Compliance/Hipaa/RPPIndividualsHipaaCEs.html (last Feb. 21, 2005).

B. DISCUSSION OF THE DOJ'S DECISION TO PROSECUTE GIBSON UNDER HIPAA

Why did the DOJ choose to prosecute Gibson under HIPAA when it could have chosen any number of seemingly more appropriate alternatives, such as identity theft or credit card fraud? HIPAA does not carry a more severe punishment than other viable options, so the choice does not seem to have been motivated by a desire to punish more harshly. U.S. Attorney Public Affairs Officer Emily Langlie explained that, "government lawyers examined the statutes that could be brought against Gibson, and it was determined that the amount of time served and penalties levied were similar whether it was tried under HIPAA or under credit card fraud laws."[74] If HIPAA was not selected because of a stiffer penalty, why charge Gibson under HIPAA? Four factors seem to have influenced this decision: 1) a connection to the health care industry, 2) an interest in deterring future HIPAA violations, 3) a desire to put the health care industry on notice that the DOJ will take HIPAA violations seriously, and 4) to indicate that individuals, and not just covered entities, may be prosecuted for violating HIPAA.

That Gibson acquired the health information in the course of his duties as a health care technician caring for Drew seems to have influenced the DOJ's decision to prosecute under HIPAA. In an interview with Susan Loitz, Assistant District Attorney for the Western District of Washington and one of the prosecutors of the *Gibson* case, Loitz stated that the DOJ "could have charged Mr. Gibson with unlawful identity theft, but the health care connection made it more important that a HIPAA crime should be charged."[75] This statement suggests that when HIPAA is an option among many, the DOJ may be more inclined to prosecute under HIPAA rather than under another statute.

A desire to deter future violations seems to have been a factor in the decision to prosecute Gibson under HIPAA. Langlie indicated that in deciding how to charge Gibson, "there is always an interest in deterrence, and this is certainly a case that had more attention than it

---

[74] Mike Scott, *HIPAA Gavel Drops – A Message to Healthcare*, RADIOLOGY TODAY, Nov. 22, 2004, at 38 *at* http://www.radiologytoday.net/archive/rt_112204p38.shtml (last Feb. 20, 2005).

[75] Alan S. Goldberg, *Interview with Susan Loitz, Assistant U.S. Attorney*, ABA HEALTH ESOURCE, Oct. 2004, *at* http://www.abanet.org/health/esource/vol1no2/ (Link to "more" for rest of article) (Last accessed on 2/20/05).

would have had it been tried under a different statute."[76] The DOJ seems to have chosen to prosecute under HIPAA with an eye towards deterring similar misuse of protected health information by both individuals and covered entities.

While deterrence may have been of significant interest to the DOJ, some health care experts argue that the *Gibson* case is unlikely to deter wrongful disclosure of individually identifiable health information by individuals who are determined to do so. American Hospital Association spokesperson Richard Wade stated, "I don't know whether the law [HIPAA] will have much of a deterrent effect on people who do that [wrongfully use individually identifiable health information]."[77] Attorney Bruce Fried of Sonnenschein Nath & Rosenthal agreed, saying that Gibson's actions are "the exact kind of behavior HIPAA was intended to go after . . . [but] greedy, stupid people will continue their scheme, even if a well-intentioned law is aimed at deterring them."[78] While deterring future HIPAA violations may have been a factor in deciding to prosecute Gibson under HIPAA, it is unclear whether the decision would in fact have the desired effect.

Numerous experts in health care law feel that a significant factor in the decision to prosecute under HIPAA may have been a desire to illustrate dramatically how seriously the government will take violations. Health care attorney Brian Annulis of Michael Best & Friedrich LLP, believes that the *Gibson* case is "the government's strongest legal message yet concerning a HIPAA infraction . . . . This was meant to send a ripple throughout the industry."[79] Dan Rode, Vice President for Policy and Government Relations for the American Health Information Management Association, called the case a "warning shot" from the government meant to attract the health care industry's attention, which it has.[80]

In addition to a desire to show how seriously the government will take HIPAA violations, the choice to charge Gibson may have been partially motivated by a desire to make clear that the DOJ will prosecute individuals, not just covered entities. Kirk Nahra speculates that, "there was some aspect of 'let's be first' in this effort by the

---

[76] Scott, *supra* note 74.

[77] Mark Taylor, *HIPAA Violator Will Serve Time,* MODERN HEALTHCARE, Nov. 15, 2004 at 17.

[78] *Id.*

[79] Scott, *supra* note 74.

[80] *Id.*

Department of Justice, as well as making the point that individuals can be prosecuted."[81] Many assumed that covered entities, and not non-covered individuals, would be prosecuted. *Gibson* showed that, at least for now, this belief was incorrect.

C. IMPLICATIONS OF THE *GIBSON* CASE

The first criminal prosecution under HIPAA carries four implications for the health care industry. First, it shows that the DOJ intends to prosecute individuals, not just covered entities. Second, it raises the question of whether covered entities will be held liable for the transgressions of their employees. Third, it could be the beginning of a trend by the DOJ towards more visible enforcement of HIPAA. And finally, it indicates that the DOJ may choose to use HIPAA to prosecute other crimes.

Before *Gibson*, many took for granted that HIPAA applied only to covered entities. In a report published in November 2003 evaluating HHS's interim enforcement rule, WEDI declared that criminal violations only apply to an individual who, "knowingly and in violation of the applicable part commits one of the offenses described [and] . . . 'person' as defined in the HIPAA legislation is limited to covered entities. Accordingly, it can be concluded that the criminal penalties set forth in the HIPAA legislation can only be applied to covered entities."[82] Health care attorney Benjamin Butler of Crowell & Moring agrees, reasoning that the law,

> arguably applies only to "covered entities," . . . who engage in electronic HIPAA transactions, so that unauthorized disclosures by others would not, by this interpretation, be violations of HIPAA. By this reasoning, unless one is a 'covered entity,' it is not obvious how one can 'violate' this part of the U.S. Code.[83]

---

[81] Kirk J. Nahra, *HIPAA Criminal Enforcement Starts* (Aug. 20, 2004), *at* http://www.wrf.com/publication.cfm?publication_id=8358 (last visited Apr. 25, 2005).

[82] WORKGROUP FOR ELECTRONIC DATA INTERCHANGE (WEDI), STRATEGIC NATIONAL IMPLEMENTATION PROCESS (SNIP): HIPAA ENFORCEMENT RULE 5, *at* http://wedi.org/cmsUploads/pdfUpload/WhitePaper/pub/Enforcement.pdf (last visited Apr. 25, 2005).

[83] Benjamin Butler, *First Ever HIPAA Privacy Criminal Conviction*, HEALTH CARE LAW IN THE NEWS (Crowell & Morning LLP) 2004,, *at* http://www.crowell.com/Content/Expertise/HealthCare/HealthCareLawNews/criminalhipaa.htm (last visited Feb. 20, 2005).

Gibson has forced the health care industry to reevaluate its assumptions regarding the applicability of HIPAA and the scope of the criminal penalties that may be imposed for its violation.

How the DOJ determined that it could prosecute individuals and not just covered entities under HIPAA is not entirely clear. Assistant U.S. Attorney Susan Loitz stated that,

> this was not a close call, by any means. We felt that Mr. Gibson clearly violated the HIPAA criminal statute. He knew what he was doing; he did what he intended to do; he was caught in the act of improperly disclosing the patient information; and so we prosecuted him under HIPAA.[84]

Loitz further revealed that "whether Mr. Gibson was or was not a covered entity under HIPAA was not of great concern to me, although I note that he is a phlebotomist who was employed by a covered entity."[85] So while the DOJ has strongly supported its interpretation of HIPAA, how it arrived at the determination that criminal penalties can be assessed against individuals as well as covered entities has yet to be clearly articulated.

D. AFTER *GIBSON*: LIABILITY FOR COVERED ENTITIES

Now that the DOJ has voiced its intention to prosecute individuals, to what extent is a non-covered individual's employer, which may be a covered entity, be held liable for the actions of an indiscriminate employee? Attorney Mark Lutes of Epstein Becker & Green P.C. predicts that providers will not be more susceptible to criminal prosecution if their employees disclose individually identifiable health information.[86] Attorney Benjamin Butler observes that "there is nothing to suggest that the Seattle Cancer Care Alliance was itself implicated in the criminal prosecution."[87]

Other legal experts are more cautious, warning that covered entities need to be vigilant as they may be held liable for the criminal actions of their non-covered employees. Attorney Michael Bell of

---

[84] Goldberg, *supra* note 75.

[85] *Id.*

[86] Taylor, *supra* note 77.

[87] Butler, *supra* note 83.

Mintz Levin in Washington, D.C., speculates that a potential reason why the Seattle Cancer Care Alliance was not pursued was because it argued that Gibson acted outside of the scope of his employment and that the Alliance should not be held responsible.[88] It should be noted that in investigating Gibson, the DOJ did review the Seattle Cancer Care Alliance's compliance policies and procedures and was satisfied that it was not culpable for Gibson's conduct.[89]

Attorney Shannon Hartsfield, who regularly advises clients on HIPAA compliance, indicates that employers could face some degree of exposure under certain circumstances. She says that, "if a workforce member violates HIPAA, covered entities could also have exposure, particularly if they have failed to conduct adequate training or develop comprehensive privacy protections. A covered entity's risks increase dramatically if it knew or should have known of an employee's improper acts."[90] HHS seems to confirm this belief, commenting in the December 2000 version of the Privacy Rule that at least for civil enforcement, "a covered entity will generally be responsible for the actions of its employees such as where the employee discloses protected health information in violation of the regulation."[91]

Covered entities can take protective measures to avoid legal responsibility for their employees' transgressions. Such measures include documentation of HIPAA compliance training for employees and complete cooperation in any investigation. When asked how attorneys can further assist their clients to avoid violating HIPAA, Loitz advised covered entities to

> [l]ook at [their] entire procedures with an eye on the purposes of the law in mind . . . [and to] deal with problems as they arise and not . . . let them pass without proper attention. Learn from your own mistakes and those of others, and don't delay making corrections to any holes that you discover in your procedures. And impose appropriate

---

[88] Youngstrom, *supra* note 73.

[89] Goldberg, *supra* note 75.

[90] Hartsfield, *supra* note 44 ¶ 3.

[91] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164), *at* http://www.hipaadvisory.com/regs/Regs_in_PDF/Final%20Privacy%20Rule.pdf at 601 (last Feb. 21, 2005).

> discipline if you discover that an employee has ignored your policies and procedures.[92]

Attorney Brian Annulis suggests that, "what you want to be able to do when the FBI or the police come to your door is cooperate with them and show them your compliance plan and how every employee has documentation of the plan."[93] Annulis further advises that employers regularly review their HIPAA compliance procedures and make clear to their employees what is and is not a violation, and what the penalties are for breaking the rules.[94]

E. WATCH FOR A LEGAL CHALLENGE TO THE PROSECUTION OF NON-COVERED INDIVIDUALS

If the Department of Justice continues to impose criminal penalties on individuals, many predict that it will be subject to a legal challenge. Attorney Kirk Nahra speculates that, "at some point in the future there will be a challenge to the government's ability to prosecute individuals who aren't covered entities for HIPAA violations."[95] Attorney Benjamin Butler agrees, stating that it is unclear how anything but a covered entity can be prosecuted for a criminal violation.[96] Butler goes on to say that the *Gibson* case did not challenge the authority of the government to prosecute Gibson individually because it ended in a guilty plea. However, future cases against individuals may challenge this practice.[97] Michael Bell calls the DOJ's actions, "a stretch of authority" and doubts that the action, if legally challenged, would have been sustained.[98]

---

[92] Goldberg, *supra* note 75.

[93] Scott, *supra* note 74.

[94] *Id.*

[95] *BNA Interviews WRF Partner Kirk J. Nahra on First HIPAA Privacy Criminal Conviction,* IN THE NEWS (Wiley Rein & Fielding LLP), August 23, 2004, *at* http://www.wrf.com/media_news.cfm?sp=news&tp=&industry_id=0&practice_ID=0&ID=1769 (last visited Apr. 25, 2005).

[96] Butler, *supra* note 83.

[97] *Id.*

[98] Youngstrom, *supra* note 73.

V. HIPAA AND THE PRIVACY RULE'S EFFECT ON PROTECTIONS FOR GENETIC INFORMATION

A. INTRODUCTION

With the final comments to the HIPAA Privacy Rule in August of 2002, as well as subsequent clarifications by HHS, new questions have arisen regarding the rule's protection of genetic information.[99] These questions regard the extent to which the Privacy Rule protects genetic information, who is restricted in their use and access to this information, and what the limitations of the HIPAA Privacy Rule are. The public seeks clarification on these issues because they fear that their privacy will be invaded, and that their genetic information will be used to discriminate against them for insurance or employment purposes.[100] HIPAA is the first federal legislation to address directly the problem of genetic discrimination, but is narrowly limited both in its protections and covered entities.[101] Thus, it becomes important to recognize and analyze HIPAA's strengths and weakness in order to develop future federal protections for genetic information.[102] Lastly, Iceland recently contracted with a private corporation to construct a database collection of their citizen's genomes.[103] While this privatization is strongly opposed in Iceland, United States legislators should closely monitor the results as it could have implications concerning future genetic privacy and nondiscrimination laws.[104] This section seeks to illustrate the extent of genetic protection under HIPAA, implications on future laws, and current events affecting the future of genetic information in the United States.

---

[99] OFFICE FOR CIVIL RIGHTS, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, YOUR FREQUENTLY ASKED QUESTIONS ON PRIVACY, *at* http://hhs.gov/ocr/hipaa/ (last revised Apr. 18, 2005).

[100] Sonia M. Suter, *The Allure and Peril of Genetics Exceptionalism*, 79 WASH. U.L.Q. 669, 673 (2001).

[101] HUMAN GENOME PROGRAM, DEPT. OF ENERGY, GENETICS PRIVACY AND LEGISLATION, *at* http://www.ornl.gov/sci/techresources/Human_Genome/elsi/legislat.shtml (last modified Oct. 19, 2004).

[102] Suter, *supra* note 100.

[103] Oksana Hlodan, *For Sale Iceland's Genetic History*, ACTIONBIOSCIENCE.ORG (June 2004) *at* http://www.actionbioscience.org/genomic/hlodan.html (last visited Apr. 25, 2005).

[104] *Id.*

B. IS GENETIC INFORMATION PROTECTED UNDER THE HIPAA PRIVACY RULE?

After the creation of HIPAA, questions persisted as to what protections would be granted for "individually identifiable health information," including questions on HIPAA's protections of genetic information.[105] These questions continued for many years until HHS answered these questions with the issuance of the Privacy Rule.[106] This Rule and subsequent HHS publications have definitively answered that "genetic information" *is* covered as "protected health information (PHI)" under the Privacy Rule.[107] Being classified as private health information under HIPAA provides protection for genetic information as it relates to "medical records and other personal health information maintained by health care providers, hospitals, health plans and health insurers, and health care clearinghouses."[108] This means that any genetic information that is "individually identifiable" pursuant to the Privacy Rule cannot be used or disclosed by "covered entities" except where the Privacy Rule permits, or as authorized by the subject of the information.[109]

While these protections are a significant step towards federal protection of genetic information, they are limited in application as well as scope.[110] HIPAA itself only applies to employer-based and commercially issued group health insurance.[111] Its notable protections for genetic information are:

- Prohibits group health plans from using any health status-related factor, including genetic information, as a

---

[105] OFFICE FOR CIVIL RIGHTS, *supra* note 26.

[106] *Id.*

[107] OFFICE FOR CIVIL RIGHTS, *supra* note 99.

[108] HUMAN GENOME PROGRAM, *supra* note 101.

[109] OFFICE FOR CIVIL RIGHTS, *supra* note 26; 45 C.F.R. § 160.103 (2005).

[110] Stephanie L. Anderson, *Genetic Privacy: A Challenge to Medico-Legal Norms Book Review*, 25 J.LEGAL MED. 119, 128-29 (2004) (feels HIPAA is a step towards federal protections, but believes that the genetic protections provided for by HIPAA are insufficient on a federal level).

[111] HUMAN GENOME PROGRAM, *supra* note 101 (see under Health Insurance Portability Act of 1996).

basis for denying or limiting eligibility for coverage or for charging an individual more for coverage

- Limits exclusions for pre-existing conditions in group health plans to 12 months and prohibits such exclusions if the individual has been covered previously for that condition for 12 months or more

- States explicitly that genetic information in the absence of a current diagnosis of illness shall not be considered a preexisting condition[112]

Although these protections are substantial, HIPAA does not prohibit insurance rate increases after genetic testing or prevent genetic discrimination by employers.[113] Likewise, it fails to prohibit employers from refusing to offer health coverage as a part of their benefit package.[114]

In conjunction with these limited protections are the restrictions on accessibility and transferability previously mentioned under the Privacy Rule. Genetic information does not receive special treatment under this rule; it simply falls within the protections granted to all private health information.[115] Furthermore, if any aspect of that information is not "individually identifiable" or is "de-identified health information," then HIPAA would not provide coverage.[116]

HIPAA and the Privacy Rule's limited applicability to "covered entities" is an additional limitation inherent in the Rule. While genetic information is restricted for "covered entities," any "business associates" not classified as a "covered entity" are not bound by the restrictions on genetic information.[117] This is especially relevant in

---

[112] *Id.*

[113] Robert A. Curley Jr. & Lisa M. Caperna, *The Brave New World is Here: Privacy Issues and the Human Genome Project*, 70 DEF. COUNS. J. 22, 29 (2003).

[114] HUMAN GENOME PROGRAM, *supra* note 101.

[115] *Id.*

[116] OFFICE FOR CIVIL RIGHTS, *supra* note 26 ("De-identified information neither identifies nor provides a reasonable basis to identify an individual.").

[117] Tamela J. White & Charlotte A. Hoffman, *The Privacy Standards Under The Health Insurance Portability and Accountability Act*, 106 W. VA. L. REV. 709, 724 (2004) ("Covered entities" are still required to contract with third parties that qualify as "business associates" to

current times, as there have been instances of genetic information being sold to private corporations for research.[118] The Privacy Rule *does* require that certain contractual protections be made between "covered entities" and "business associates," but only "covered entities" can be held liable for misuse of information by "business associates."[119] Additionally, only third parties who do business with "covered entities" *as well as* function for or on their behalf will be considered a "business associate" pursuant to the Privacy Rule.[120] This means that covered entities doing business with third parties who do not qualify as "business associates" under the Privacy Rule, are not personally liable for any misuse of that information by the third party.[121]

As previously mentioned, the Privacy rule also permits both authorized and un-authorized disclosures depending upon the circumstances surrounding the disclosure. Examples of situations in which authorization is not required include medical treatment, public interest, or limited research.[122] In addition to these permitted "unauthorized disclosures," covered entities are also permitted *authorized* disclosures for private health information that is not otherwise permitted or required by the Privacy Rule.[123] This has significant implications when dealing with genetic information due to the massive index of information available about one's entire family from a single sample of genetic information.[124] It appears that HHS has addressed this issue in its recent comments to the Privacy Rule. In these comments HHS indicates that such information would be

---

ensure protections of PHI. However, it is the covered entity who remains liable in the case of a violation).

[118] *See* discussion *infra* Part V.C. on Iceland deCode experience.

[119] OFFICE FOR CIVIL RIGHTS, *supra* note 26; 45 C.F.R. §§ 164.502(e), 164.504(e) (2005).

[120] Nancy A. Lawson et al., *The HIPAA Privacy Rule: An Overview of Compliance Initiatives and Requirements,* 70 DEF. COUNS. J. 127, 140 (2003).

[121] *Id.*

[122] OFFICE FOR CIVIL RIGHTS, *supra* note 26, *at* 4 (provides extensive list on permitted non-authorized disclosures).

[123] *Id.* at 9.

[124] Anita Silvers & Michael Ashley Stein, *Human Rights and Genetic Discrimination*, 31 J.L. MED. & ETHICS 377, 378 (2003).

protected as long as it meets the requirements of the Rule.[125] The practicality of this is questionable as it would be difficult to determine who has a *greater* right to privacy, or who would benefit more from disclosure versus protection.[126]

Issues with applicability continue to persist with business associates and unclassifiable third party businesses. In addition, there are continuing concerns about *any* access to genetic information due to the scope of information accessible through even limited access. Thus, although genetic information is definitely protected under the Privacy Rule, the extent of such protections remains to be seen.

C. APPROACHES TO FUTURE GENETIC PROTECTION LEGISLATION

It is still too early to determine the success and/or shortcomings of the protections granted by HIPAA and the Privacy Rule. Nonetheless, the limitations inherent in HIPAA suggest further federal protections are needed to prevent genetic discrimination in *individual* insurance coverage, as well as genetic discrimination in the workplace.[127] These areas are of great concern because the public fears that "1) insurers will use genetic information to deny, limit, or cancel insurance policies or 2) employers will use genetic information against existing workers or to screen potential employees."[128] Scholars and professionals continue to interpret the implications of HIPAA, while recognizing a growing awareness that further protections for genetic information *are* needed.[129]

1. GENETIC EXCEPTIONALISM

One of the main debates regarding future protections for genetic information centers on whether genetic protections should treat genetic information as an exception to, or consistent with other private health information.[130] As previously discussed, the Privacy Rule treats

---

[125] Anderson, *supra* note 110, at 129 (citing 65 Fed. Reg. 82462 (Feb. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164)).

[126] Silvers & Stein, *supra* note 124.

[127] HUMAN GENOME PROGRAM, *supra* note 101.

[128] *Id.*

[129] Curley & Caperna, *supra* note 113.

[130] *Id.*

genetic information consistently with all other private health information.[131] Some scholars and professionals believe that this approach is the correct approach to apply to future federal protections of genetic information.[132] This approach is appealing because it avoids problems of over and under inclusiveness when laws are created to protect only certain types of information.[133] Scholars believe that by creating broad based protections for all private health information (including genetic information), no class inequities will result from genetic exceptionalism, which inherently creates differentiating restrictions between classes of people.[134]

2. PRIVACY BASED PROTECTIONS

Regardless of the classification of genetic information, debates continue on whether future laws should use a *privacy* based or *anti-discrimination* based approach to protect genetic information.[135] Proponents of the privacy-based approach believe that federal laws protecting genetic information should be based upon protecting "an individual's autonomy to control her own destiny."[136] The strength of this approach lies with privacy protections already guaranteed in the Fourth, Fifth, and Fourteenth amendments of the United States Constitution.[137] In addition, privacy based protections already exist in twenty-four of the states.[138] A common practice with privacy legislation is to require consent when accessing a person's genetic information.[139] Thus, where privacy legislation has been enacted, the

---

[131] HUMAN GENOME PROGRAM, *supra* note 101.

[132] Suter, *supra* note 100, at 742–43.

[133] *Id.* at 709–15.

[134] *Id.* at 747.

[135] Silvers & Stein, *supra* note 124.

[136] *Id.*

[137] *Id.*

[138] NATIONAL CONFERENCE OF STATE LEGISLATURES, STATE GENETIC PRIVACY LAWS, *at* http://www.ncsl.org/programs/health/genetics/prt.htm (last visited Feb. 20, 2005).

[139] Silvers & Stein, *supra* note 124.

focus is on building trusting relationships where disclosures are voluntary and remain within the control of the individual.[140]

The strength and weakness with the privacy approach is its isolated focus on requiring consent to access genetic information. This focus often fails to adequately consider public policy concerns and the unique intrusive nature of genetic information.[141] Namely, this approach fails to recognize that a person's genetic information can be used to determine their entire families' genetic information.[142] Where a person gives permission to disclose his or her genetic information, they would presumably be granting permission for all persons whose information could be ascertained by the original sample.[143] In this situation, requiring consent from one person would inadequately protect the entire family's interest. Furthermore, some scholars believe that it may be a legal fiction that supervisors, insurers, or employers permitted to use this information would limit their use to the intended purpose (i.e. not for employment or insurance premium/coverage purposes).[144] Thus, fears persist that once access has been granted to one's genetic information, the information could be used later in life in a discriminatory fashion.[145]

These privacy concerns have only grown in recent years with developments in the Human Genome Project.[146] While this was a landmark achievement, greater knowledge of the human genome also means greater ability to differentiate and discriminate against variations identified in the genome.[147] This is an especially relevant

---

[140] Sonia M. Suter, *Disentangling Privacy from Property*, 72 GEO. WASH. L. REV. 737, 812 (2004).

[141] Silvers & Stein, *supra* note 124.

[142] *Id.*

[143] *Id.*

[144] *Id.*

[145] *Id.*

[146] NATIONAL HUMAN GENOME RESEARCH INSTITUTE, NATIONAL INSTITUTES OF HEALTH, PRIVACY OF GENETIC INFORMATION, *at* http://www.genome.gov/10002336 (last updated Apr. 2005).

[147] *Id.*

topic in Iceland where genome research is being conducted on the largely homogenous Icelandic population.[148]

In December of 1998, the Icelandic parliament passed a bill ordering the creation of a national database of all Icelandic people's genetic and personal health information.[149] The parliament then granted an exclusive contract to create this database to a biomedical company called deCode genetics.[150] deCode genetics then proceeded to contract with Hoffman-LaRoche, a pharmaceutical company, in order to finance certain genetic research.[151] As a result of these contracts, the Icelandic people's genetic information has been disclosed to private entities for genealogical research.[152] Recently, deCode genetics declared that the genealogical database of all Icelandic citizens was almost finished, and would be published on the Internet when completed.[153]

This privatization and open access to Iceland's citizens' genealogical data creates ethical, legal, and business concerns.[154] The Association of Icelanders for Ethics in Science and Medicine (Mannvernd) strongly opposed its government's actions and sought to have this Health Sector Database stricken as unconstitutional.[155] This goal became a reality in November 2003, when the Icelandic Supreme Court addressed the constitutionality of the database.[156]

---

[148] Hlodan, *supra* note 103.

[149] *Id.*

[150] *Id.* FAQs regarding this project are posted at http://www.decode.com.

[151] *Id.* (Research on heart attacks, emphysema and Alzheimer's).

[152] *Id.*

[153] Hlodan, *supra* note 103. deCode plans to market its information for a fee to interested parties, including pharmaceutical and health insurance companies. *Id.*

[154] *Id.* (*See* subtopic *Why there is opposition to this project*).

[155] ASSOCIATION FOR ICELANDERS FOR ETHICS IN SCIENCE AND MEDICINE, MANNVERND, LATEST NEWS AND ARTICLES, *at* http://www.mannvernd.is/english/home.html (last updated Apr. 25, 2005).

[156] Gudmundsdottir v. State of Iceland, No. 151/2003 (Icelandic Supreme Court Nov. 27, 2003), *available at* http://www.mannvernd.is/english/lawsuits/Icelandic_Supreme_Court_Verdict_151_2003.pdf (last visited Apr. 25, 2005).

In this landmark case, the plaintiff sought to prevent the transfer of data belonging to her deceased father to the Health Sector Database.[157] She argued that this data concerned certain aspects of her own genome, which gave her a right to refuse consent to include it within the national database.[158] The Court agreed with the plaintiff and struck down the HSD Act as unconstitutional.[159] This holding has worldwide implications as it recognizes a willingness to extend genetic privacy protections to all those who may have a genetic interest in the disclosure or access to such information.[160]

Legislators in the United States would be wise to consider the events in Iceland as an outline for creating privacy-based legislation. While the Privacy Rule provides *some* protections in limited circumstances, it fails to provide sufficient protections to protect against situations similar to that in Iceland. The Icelandic government made deals with private companies who under the Privacy Rule (assuming it applied in Iceland), would have been considered either "business associates" or uncovered entities. In the United States, companies like deCode would be only partially liable for their business associates' infractions, or not liable at all if these associates were not considered "business associates" pursuant to the Privacy Rule.[161] This illustrates a disturbing scenario in which private non-covered entity companies could both disclose and benefit from an individual's genetic information.[162] While the Iceland situation is a victory for privacy-based protections, it also illustrates that further protections are needed when genetic information is disclosed.

---

[157] *Id.*

[158] *Id.*

[159] *Id.*

[160] Press Release, Association for Icelanders for Ethics in Science and Medicine, Icelandic Supreme Court's Nov. 27, 2003 Decision *at* http://www.mannvernd.is/english/lawsuits/Mannvernd_PressRelease_SupremeCourt.html (last visited February 20, 2005).

[161] White & Hoffman, *supra* note 117, at 731-32.

[162] Hlodan, *supra* note 103 (In Iceland, deCode has a monopoly on the genetic data and is permitted to commercialize the data for twelve years.).

3. ANTI-DISCRIMINATION APPROACH

The privacy based approach to genetic information protections focuses on trusting relationships and requiring consent for disclosures.[163] However, the anti-discrimination model assumes that the privacy model will be unsuccessful, and provides regulations for how this information should and should not be used.[164] To date, there has been no specific federal genetic nondiscrimination legislation enacted.[165] While HIPAA directly addresses certain genetic discrimination practices, it was not created for the sole purpose of preventing genetic discrimination.[166] Therefore, *existing* nondiscrimination laws have occasionally been interpreted to provide protections against genetic discrimination.[167]

The Americans with Disabilities Act[168] is one of the commonly argued laws granting protections against genetic discrimination.[169] The ADA does not directly prohibit genetic discrimination, but it does provide "some protections for disability related discrimination in the workplace."[170] Many have argued that this means the ADA would cover disability discrimination based upon a genetic condition.[171] This argument has, however, been called into doubt by a United States Supreme Court decision.[172] In *Bragdon* v. *Abbott*, Chief Justice Rehnquist's dissent suggested that he may be reluctant to define individuals with genetic alterations as disabled pursuant to ADA.[173] Subsequent Supreme Court decisions have been consistent with this

---

[163] Suter, *supra* note 140.

[164] Silvers & Stein, *supra* note 124, at 379.

[165] HUMAN GENOME PROGRAM, *supra* note 101.

[166] 45 C.F.R §§ 160, 162, 164 (2005).

[167] HUMAN GENOME PROGRAM, *supra* note 101.

[168] 42 U.S.C.A. § 12101.

[169] *Id.*

[170] Curley & Caperna, *supra* note 113, at 30.

[171] *Id.*

[172] Bragdon v. Abbott, 524 U.S. 624, 657-62 (1998).

[173] Curley & Caperna, *supra* note 113. *See also Bragdon*, 524 U.S. at 657.

opinion and have further limited the protected class under the ADA as a matter of policy.[174]

Absent the ADA and HIPAA's restrictions on genetic discrimination, there appears to be a lack of broad anti-discrimination laws on the federal level.[175] HIPAA and its Privacy Rule provide a good example of a mixture of privacy and anti-discrimination based laws, but is insufficient to provide a national standard for medical and/or genetic privacy.[176] Due to this lack of federal protections for genetic information, U.S. citizens are left to their individual state's privacy laws for protection from invasion of privacy and genetic discrimination.[177]

D. THE FUTURE OF PRIVACY AND ANTI-DISCRIMINATION PROTECTIONS

In 2001, legislation was introduced by Senator Tom Daschle and House Representative Louise Slaughter, which would provide protection for genetic information that was not otherwise provided for by HIPAA.[178] The foundation of this act was established after the February 8, 2000 executive order prohibiting *federal* employers from considering genetic information in employment decisions.[179] The act entitled "Genetic Nondiscrimination in Health Insurance and Employment Act," prohibits insurers from using protected genetic information to make decisions about eligibility for group or *individual* health plans, or to make premium adjustments in light of such information.[180] Additional protections include restrictions on insurers' access to private genetic information, as well as strict prohibitions on genetic discrimination in employment situations.[181] It appears that this

---

[174] Sutton v. Airlines, Inc., 527 U.S. 471 (1999).

[175] HUMAN GENOME PROGRAM, *supra* note 101.

[176] Anderson, *supra* note 110.

[177] *Id.* States' varying protections concerning genetic information will be discussed more thoroughly in the subsequent section. *See* discussion *infra* Part VI.

[178] CENTER FOR SCIENCE AND TECHNOLOGY IN CONGRESS, AMERICAN ASSOCIATION FOR THE ADVANCEMENT OF SCIENCE STATUS OF MAJOR LEGISLATION, *at* http://www.aaas.org/spp/cstc/stc/status.htm (last updated Feb. 28, 2001).

[179] Curley & Caperna, *supra* note 113, at 30.

[180] Suter, *supra* note 100, at 697.

[181] *Id.*

legislation would patch many of the holes in the current protections, while meeting the twin goals of protecting individual privacy and prohibiting genetic discrimination. However, this legislation continues to be considered in committee while attempts are made to agree on its provisions.[182]

Similarly, numerous genetic nondiscrimination and privacy bills have been introduced to Congress, but continue to be considered in Congressional committees.[183] While these bills are being refined and eliminated, individuals are forced to rely on limited HIPAA protections as well as their own state laws. This state dependent scheme provides varied genetic coverage and protections, but generally prohibits employers from requiring workers and applicants to undergo genetic testing as a condition of employment.[184] This provides confusion from state to state, but individuals can find their states' genetic privacy laws on the National Conference of Legislatures website.[185]

There is no definitive answer as to what future federal protections will be granted for genetic information. Until pending legislative protections are enacted by Congress, individuals must rely on the existing federal protections under HIPAA, in addition to their home state's protections

E. CONCLUSION

HIPAA and the Privacy Rule have ensured specific privacy protections for an individual's genetic information, while also federally barring genetic discrimination with group insurance practices. These protections, though limited, have provided legislators with invaluable experience in developing the proper approach to genetic privacy and nondiscrimination. It appears that future

---

[182] Release, Senator Tom Daschle, Statement by Leader Daschle on Help Committee Reporting out the Genetic Nondiscrimination Bill (May 21, 2003) (regarding the status of the bill), *at* http://democrats.senate.gov/~dpc/releases/2003522A49.html (last visited Apr. 25, 2005).

[183] HEALTH PRIVACY PROJECT, 108TH CONGRESS HOUSE BILLS, *at* http://www.healthprivacy.org/newsletter-url2305/newsletter-url.htm (last visited Apr. 25, 2005); HEALTH PRIVACY PROJECT, 108TH CONGRESS SENATE BILLS, *at* http://healthprivacy.org/newsletter-url2305/newsletter-url.htm (last visited Apr. 25, 2005).

[184] HUMAN GENOME PROGRAM, supra note 101 (see *State Policy History*).

[185] NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 138.

legislation should ensure an individual's right to privacy, while guaranteeing protections if that privacy is breached. Additionally, current events in Iceland illustrate valid concerns with the use of genetic information. Thus, using the strengths of HIPPA and the Privacy Rule, and correcting their weaknesses, further federal protections for genetic information can become a reality.

VI. STATE COMPLIANCE AND THE DISPARITY IN STATE PRIVACY LAW

A. INTRODUCTION

One of the largest areas of confusion regarding HIPAA and the Privacy Rule is how these statutes interact with state laws concerning privacy.[186] However, this issue has become less confusing as the Department of Health and Human Services has recently published FAQs and a Summary of the Privacy Rule on its website.[187] Generally, the Privacy Rule preempts all conflicting state laws, unless the state law requires stricter privacy restrictions than the Privacy Rule.[188] Although this seems like a simple test, problems continue as various exceptions to the rule complicate compliance.[189] Additional difficulties lie in attempting to comply with various state and federal laws, without endangering compliance with the Privacy Rule. Where state law governs, variations in state protections make it extremely difficult to determine what privacy laws govern. This confusion, combined with a lack of federal support, demands federal attention to remedy disparate protections amongst the states. Thus, where HIPAA fails to preempt state law, federal legislation is needed to provide uniform protection.

B. PRE-EMPTION POLICY

After the August 14, 2003 deadline for compliance with the Privacy Rule, states and "covered entities" have experienced

---

[186] Steve Fox & Rebekah A.Z. Monson, *Interaction of HIPAA with State and Other Federal Laws*, HIPAA/LAW: LEGAL Q/A (Phoenix Health Systems, Washington, D.C.) Sept. 2004, *at* http://www.hipaadvisory.com/action/legalqa/hipaalaw.htm (last visited Feb. 20, 2005).

[187] OFFICE FOR CIVIL RIGHTS, *supra* note 99; OFFICE FOR CIVIL RIGHTS, *supra* note 26.

[188] OFFICE FOR CIVIL RIGHTS, *supra* note 26 (citing 45 C.F.R §160.203 2005)).

[189] *Id.*

difficulties in determining their compliance with the Rule.[190] The general policy established in the Privacy Rule is that "State laws that are contrary to the Privacy Rule are preempted by the federal requirement, which means that the federal requirements will apply."[191] HHS further defines "contrary" laws, as those laws which are impossible to comply with, without hindering an entity's ability to comply with HIPAA or some purpose or objective of HIPAA.[192] The Privacy Rule is simply meant to establish a uniform "floor" of protection for protected health information.[193]

Nonetheless, the Privacy Rule provides exceptions to this preemption policy for contrary state laws that: 1) relate to the privacy of the individually identifiable information and provide *greater* privacy protections or privacy rights with respect to such information, 2) "provide for the reporting of disease or injury, child abuse, birth, or death," or for public surveillance, investigation, or intervention, or 3) require certain health plan reporting.[194] In addition to these exceptions, the Privacy Rule provides additional exceptions for state laws where specific situations or public interests are involved.[195]

The problem with this standard is that "covered entities" are still confused as to whether their state laws are more stringent than the HIPAA Privacy Rule.[196] HHS has again attempted to clarify this issue by defining factors for an entity to consider when determining whether their state law preempts the Privacy Rule. These factors are:

- Whether disclosure or use are restricted when otherwise allowed under the Privacy Rule;
- Whether state restrictions limiting access to PHI provide greater restrictions than the Privacy Rule;

---

[190] *Id.*

[191] *Id.*

[192] *Id.*

[193] HEALTH PRIVACY PROJECT, INSTITUTE FOR HEALTHCARE RESEARCH AND POLICY GEORGETOWN UNIVERSITY, SUMMARY OF HIPAA PRIVACY RULE 34 (2002), *at* http://www.healthprivacy.org/usr_doc/RegSummary2002.pdf (last visited Apr. 25, 2005).

[194] *Id.*

[195] *Id.*

[196] OFFICE FOR CIVIL RIGHTS, *supra* note 99.

- Whether state laws require stricter form or substance when obtaining legal permission for disclosures of identifiable health information, or

- Whether any additional protections are granted to an individual, not otherwise available under the Privacy Rule.[197]

In addition to these and other clarifications published by HHS, many state bar and other associations provide HIPAA preemption matrices in order to assist covered entities to achieve compliance.[198] Although this preemption analysis can be challenging, professionals believe that a compliant blending individual state, HIPAA, and other privacy laws is possible.[199]

C. EXAMPLES AND DIFFERENCES IN STATE PRIVACY PROTECTIONS

When a state's privacy law preempts the Privacy Rule, or privacy issues do not fall within the purview of the Rule, individuals must rely solely on their state's privacy protections.[200] However, every state has varying privacy protections depending upon the use and access to private information.[201] Thus, if both the state and HIPAA fail to provide protection, a person may find himself or herself without certain privacy protections.

This varying degree of protection is illustrated by the states' wide range of genetic privacy laws. Most states have privacy laws that treat genetic information separately from other private health information, e.g., genetic exceptionalism.[202] Washington is the only state that treats

---

[197] 45 C.F.R. § 160.202 (2005).

[198] PHOENIX HEALTH SYSTEMS, STATE AND FEDERAL PRIVACY LAWS AND PREEMPTION ANALYSES, *at* http://www.hipaadvisory.com/regs/StateLaws.htm (last visited Apr. 25, 2005) (Ohio and Washington Matrices).

[199] Fox, *supra* note 185.

[200] White & Hoffman, *supra* note 117, at 727.

[201] HEALTH PRIVACY PROJECT, STATE HEALTH PRIVACY LAWS (2d ed. 2002) (List privacy laws for all fifty states), *available at* http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm (Last viewed February 20, 2005).

[202] NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 138.

genetic information the same as all other protected health information.[203] The Privacy Rule follows a similar approach in treating genetic information no differently than other private health information.

Most state privacy laws prevent certain parties from accessing or using private information in certain capacities.[204] Twenty-four states require informed consent to disclose genetic information, while Rhode Island and Washington have an additional requirement of written authorization to disclose the same information.[205] Furthermore, Alaska, Colorado, Florida, Georgia, and Louisiana classify genetic information as property of the individual.[206] This classification of genetic information is significant, because it completely changes the justification for the protections. Most privacy laws focus on protecting personal autonomy and the right to privacy. States creating this property right, however, can argue for privacy protections under the guise of property law.

Privacy laws are also enforced in varying degrees depending on the state. Eighteen states have criminal penalties, civil penalties, or both, for violations of their genetic privacy laws.[207] The remaining states create no specific penalty for similar violations.[208] This is a significant difference that could create inequities for the same violations in different states.

State genetic privacy laws also vary protections in employment situations. Thirty-two states currently enforce genetic nondiscrimination laws, but differ in the extent of their protections.[209] Some states strictly prohibit genetic testing, while others simply restrict an employer's access to genetic information.[210] For the moment, employment is an area where an individual is largely

---

[203] *Id.*

[204] *Id.*

[205] *Id.*

[206] *Id.*

[207] NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 138.

[208] *Id.*

[209] NATIONAL CONFERENCE OF STATE LEGISLATURES, STATE GENETICS EMPLOYMENT LAWS, *at* http://www.ncsl.org/programs/health/genetics/ndiscrim.htm (last visited Apr. 25, 2005).

[210] *Id.*

dependent on the law of his or her state to provide protections against genetic discrimination.[211] This is subject to change if pending federal employment protections are enacted.[212]

In situations where HIPAA and the Privacy Rule do not apply nor preempt state law, privacy protections for genetic information may vary when used in health insurance. "These laws may restrict health insurers from engaging in certain activities, including using genetic information to determine eligibility or set premiums, requiring genetic testing of applicants, or disclosing genetic information without consent."[213] It is important to note, that while HIPAA provides coverage for employer-sponsored health benefit plans, *individuals* must still rely on *state* protections for genetic information.[214]

These examples illustrate the great disparity between existing genetic privacy laws. Due to this disparity in privacy protections, U.S. citizens are at risk of receiving various degrees of genetic privacy protections as well as varying penalties for similar violations. This problem of varying protections is not limited to genetic information, but is ubiquitous throughout state privacy law.[215] HIPAA has achieved its goal of creating a "floor" of specific privacy protections in the insurance arena. These protections, however, must now be expanded in order to address disparities in state laws dealing with nondiscrimination and privacy.

D. CONCLUSION

The first dilemma facing "covered entities" under the Privacy Rule is determining whether the Privacy Rule preempts their state law. This is a confusing examination of state and federal law, but has becomes easier with guidance from HHS and professionals, who now have experience after the 2003 compliance deadline. As this preemption

---

[211] *Id.*

[212] HEALTH PRIVACY PROJECT, STATE HEALTH PRIVACY LAWS (2d ed. 2002), *available at* http://www.healthprivacy.org/newsletter-url2305/newsletter-url.htm (Last viewed May 8, 2005).

[213] NATIONAL CONFERENCE OF STATE LEGISLATURES, STATE GENETICS AND HEALTH INSURANCE STATE ANTIDISCRIMINATION LAWS, *at* http://www.ncsl.org/programs/health/genetics/ndishlth.htm (last visited Apr. 25, 2005).

[214] *Id.*

[215] HEALTH PRIVACY PROJECT, *supra* note 201.

policy becomes clearer, however, entities are faced with the reality of varying privacy protections between states. Nowhere is this more noticeable than with the great disparity of genetic information protections amongst the states. Pending federal legislation seeks to provide greater and more uniform privacy protections to remedy these disparities. In the meantime, for better or worse, United States citizens must rely on their state's privacy protections, supplemented by a "floor" of entity-limited privacy protections under the Privacy Rule.

VII. CONCLUSION

Since the release of the Privacy Rule, numerous questions have arisen concerning its scope, interpretation, and enforceability. Many question whether the Privacy Rule is being enforced, as OCR has not assessed any civil monetary penalties for a violation, even though it has received thousands of complaints. While enforcement seemed sluggish in 2004, due in part to OCR's focus on voluntary compliance and the low quality of some of the complaints, it is likely to become more vigorous in the near future, as people become more educated about the Rule and as OCR investigations progress through the enforcement pipeline.

There is also a looming question of whether the Privacy Rule may properly be enforced against individuals as it was in the *Gibson* case. The DOJ's choice to prosecute Gibson caused a ripple in the health care industry, and it is likely to be challenged in the near future.

Another prominent question is the extent of protection the Privacy Rule provides for an individual's genetic information. It appears that HIPAA and the Privacy Rule cover such information, but the protection is limited. How to protect genetic information will likely become a hotly debated issue as future legislation defines the scope of such protection.

In addition, covered entities continue to struggle with the challenge of determining whether the Privacy Rule preempts their state laws, and what protections these laws guarantee. This assessment will become easier in 2005 as HHS, pending legislation, and the courts continue to provide guidance.